UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,790	10/19/2005	Francesco Pessolano	NL030397US1	4003

65913 7590 04/01/2010

NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
KING, JOHN B	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
04/01/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	**Application No.** 10/553,790	**Applicant(s)** PESSOLANO, FRANCESCO	
	Examiner John B. King	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 10-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 10-14* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on December 18, 2009.

2. Claims 1-8 and 10-14 are pending in this application.

3. Applicant's arguments in respect to Claims 1-8 and 10-14 have been considered but they are not fully persuasive.

Response to Arguments

4. Applicant's arguments filed December 18, 2009 have been considered but they are not fully persuasive. In the remarks applicant argues:

I) The combination of Thüringer and Odinak.

In response to applicant's arguments:

I) In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Thüringer discloses one way to mask power supply fluctuations and Odinak discloses a different way to mask the power supply fluctuations. It would be obvious to replace one with the other. This would result in the output power supply being random instead of constant.

Examiner Notes

5. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claims 1 and 7** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claims 1 and 7 recite the limitation “each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits” which, based on applicant’s arguments, is unclear and ambiguous. It is unclear if this limitation

means that the processing circuit contains an input and output signal if the circuit is arranged as a feedback loop system.

9. The examiner has cited particular examples of 35 U.S.C. 112 rejections above. It is respectfully requested that, in preparing responses, the applicant check the claims for further 35 U.S.C. 112 rejections as being indefinite in the event that it was inadvertently missed by the examiner. The following prior art rejections are based upon the examiner's best interpretation of the claims.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claims 1 and 5-7, 8-14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Thüringer et al. (US 6498404 B1), published December 24, 2002 hereinafter referred to as Thüringer in view of Odinak (US Patent 6419159) and further in view of Applicant's Admitted Prior Art (AAPA) paragraphs 3-5.

As per claim 1, Thüringer discloses an electronic circuit device for executing operations dependent on secret information, the electronic circuit device, comprising: power supply connections **(col. 1 lines 28-32 and col. 2 lines 28-30, Thüringer teaches the use of power supplies.)**; a processing unit **[circuit arrangement]** comprising a plurality of processing circuits for use in execution respective parts of the operations dependent on the secret information **(col. 1 lines 45-52, Thüringer teaches a circuit arrangement for performing security-relevant operations where the security-relevant operations involve processing secret information as indicated in col. 2 lines 62-67 through col. 3 lines 1-6. Thüringer, Figure 2, discloses a plurality of processing circuits such as the AND gates.)**, the processing circuits being fed from the power supply connections **(Figure 2, Thüringer teaches having a set of AND gates. It is inherent that the AND gates are connected to the power supply in order for the circuit to work.)**; an activity monitor circuit coupled to receive pairs of processing signals, each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits **(Figure 2, Thüringer teaches a circuit that takes in a pair of signals and then outputs a pair of signals after processing. Thüringer, col. 2 lines 39-45, discloses the inputting and outputting of Figure 2.)**, the activity monitor circuit being arranged to derive activity information derived from each pair of processing signals, the activity information indicative of whether each of the processing circuits generates a logic level transition **(col. 2 lines 47-60, Thüringer teaches the circuit determining if the incoming logic signals are**

high or low.), and to derive from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals **(col. 1 lines 46-65, Thüringer teaches the load circuit being controlled by what happens in the other parts of the circuit device. Thüringer, col. 1 lines 46-52, teaches that the load circuit produces a current to be complementary to the rest of the circuit. Therefore, the load current is being added to the current that the remainder of the circuit is using to prevent third parties from determining the secret information by measuring the power consumed by the device.)**; a current drawing circuit connected to the power supply connections and controlled by the activity monitor circuit to draw a cloaking current controlled by the combined activity signal **(col. 1 lines 28-38, Thüringer teaches having a load circuit connected to the power supply to mask the measurable power consumption. Thüringer, col. 1 lines 46-65, teaches the load circuit being complementary to the other parts of the circuit. The AND gates process the incoming signals to generate the complement to be used to control the load circuit.)**, so that power supply current variations dependent on the secret information are cloaked in a combination of the cloaking current and current drawn by the processing circuits **(col. 1 lines 46-52, Thüringer teaches that the load circuit produces a current to be complementary to the rest of the circuit. Therefore, the load current is being added to the current that the remainder of the circuit is using.)**

However, Thuringer does not specifically teach having multiple processing circuits and combining the results from the multiple processing circuits to generate an overall result.

Odinak teaches having multiple processing circuits and combining the results from the multiple processing circuits to generate an overall result **(Odinak, col. 2 lines 12-26, teaches having multiple current sinks that randomly turn on and off. The combination of the current from all current sinks produces a cloaking current that is not dependant on any secret information. This cloaking current is then used to mask the normal power fluctuations that could be used to determine the secret information.)**

Thuringer and Odinak are analogous art because they are from the same field of endeavor of masking a power supply to prevent an attacker from performing power analysis on the system to determine the secret information being processed by the system. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Thuringer by adding the teachings of Odinak because this would increase the security of the system by making the output power supply based on the randomness of the current sinks instead of making the output power supply constant as in Thuringer. It would also be obvious to have multiple circuits perform the same task as a single circuit as long as the output is the same in both cases with the same input.

However, Thüringer does not specifically disclose the use of a feedback loop system to perform the claimed features.

AAPA discloses each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits **(AAPA, paragraph 5, teaches the use of a feedback loop system to keep the power supply current constant to prevent the unauthorized access to the encryption key.)**, the activity information indicative of whether each of the processing circuits generates a logic level transition **(AAPA, paragraphs 3 and 4, also teach monitoring the activity level of a cryptographic circuit by monitoring the logic level changes of the circuit.)**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Thüringer by adding the teachings of AAPA. Thüringer teaches masking the power supply current by using a loading circuit. AAPA, paragraphs 3-5, teach masking the power supply current by monitoring the logic level changes of the circuit and also by using a feedback loop system. All of these systems are used to mask the power supply current to prevent the unauthorized access to the encryption information that is used in the circuit. It would have been obvious to use one system instead of another or to combine the systems to make it even more secure.

As per claim 5, Thüringer in view of Odinak and AAPA discloses an electronic circuit device according to claim 1 **[See rejection to claim 1 above]**, having a trigger input coupled to the current drawing circuit **(Thüringer, Figure 3 and col. 3 lines 17-23, teaches having a voltage signal, V, connected to the switching transistors to control the load resistors.)**, arranged to enable drawing of the cloaking current only upon receiving a trigger signal that triggers or accompanies execution of a secret information dependent process in the electronic circuit device **(Thüringer, Figure 3 and col. 3 lines 17-23, teaches having transistors connected to the load circuit resistors. Therefore, the load current will only be drawn when the transistors are switched on, when the voltage V signal is high.)**

As per claims 6, 8 and 14, Thüringer in view of Odinak and AAPA discloses a reference current pattern generator, the current drawing circuit being arranged to adjust the value of the cloaking current so that the combination of the cloaking current and current drawn by the processing circuits substantially equals a temporal reference current pattern generated by the reference current pattern generator **(col. 1 lines 53-55, Thüringer teaches keeping the measurable power consumption constant.)** The concepts and advantages of using a reference pattern is well known and expected in the art. For example, U.S. Patent number US 4212056 describes comparing a detected signal to a reference current pattern to vary the pulse width in a PWM (Pulse Width Modulation) system (see col. 6 lines 45-50). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to generate a reference current pattern, compare the reference current pattern to another current signal, and modify that current signal to match the reference current pattern.

As per claim 7, Thüringer discloses a method of executing operations dependent on secret information in an electronic circuit, the method comprising: supplying power supply current to processing circuits **(col. 1 lines 28-32 and col. 2 lines 28-30, Thüringer teaches the use of power supplies.)**; executing respective parts of operations that dependent on the secret information using the processing circuits **(col. 1 lines 45-52, Thüringer teaches a circuit arrangement for performing security-relevant operations where the security-relevant operations involve processing secret information as indicated in col. 2 lines 62-67 through col. 3 lines 1-6.)**; receiving pairs of processing signals coming into and out of respective ones of the processing circuits, each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits **(Figure 2, Thüringer teaches a circuit that takes in a pair of signals and then outputs a pair of signals after processing. Thüringer, col. 2 lines 39-45, disclose the inputting and outputting of Figure 2.)**; deriving activity information from each pair of processing signals, the activity information indicative of whether each of the processing circuits generates a logic level transition **(col. 2 lines 47-60, Thüringer teaches the circuit determining if the incoming logic signals are high or low.)**, deriving from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals **(col. 1 lines 46-65, Thüringer teaches the load circuit being controlled by what happens in the other parts of the circuit device. Thüringer, col. 1 lines 46-52, Thüringer teaches that the load circuit produces a current to be complementary to the rest of the circuit. Therefore, the load current is being added to the current that the remainder of the circuit is using. Thüringer, col. 1 lines 33-37, also teaches that**

the measure power consumption will be the combination of the power drawn by the data processing device and the excess power drawn by the load circuit.); drawing a cloaking current controlled by the combined activity signal **(col. 1 lines 28-38, Thüringer teaches having a load circuit connected to the power supply to mask the measurable power consumption. Thüringer, col. 1 lines 46-65, teaches the load circuit being complementary to the other parts of the circuit. The AND gates process the incoming signals to generate the complement to be used to control the load circuit.)**, and combining that cloaking current with current drawn by the processing circuits so that power supply current variations dependent on the secret information are cloaked in the combination of the cloaking current and current drawn by the processing circuits **(col. 1 lines 46-52, Thüringer teaches that the load circuit produces a current to be complementary to the rest of the circuit. Therefore, the load current is being added to the current that the remainder of the circuit is using.)**

However, Thuringer does not specifically teach having multiple processing circuits and combining the results from the multiple processing circuits to generate an overall result.

Odinak teaches having multiple processing circuits and combining the results from the multiple processing circuits to generate an overall result **(Odinak, col. 2 lines 12-26, teaches having multiple current sinks that randomly turn on and off. The combination of the current from all current sinks produces a cloaking current that is not dependant on any secret information. This cloaking current is then used to**

mask the normal power fluctuations that could be used to determine the secret information.)

Thuringer and Odinak are analogous art because they are from the same field of endeavor of masking a power supply to prevent an attacker from performing power analysis on the system to determine the secret information being processed by the system. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Thuringer by adding the teachings of Odinak because this would increase the security of the system by making the output power supply based on the randomness of the current sinks instead of making the output power supply constant as in Thuringer. It would also be obvious to have multiple circuits perform the same task as a single circuit as long as the output is the same in both cases with the same input.

However, Thüringer does not specifically disclose the use of a feedback loop system to perform the claimed features.

AAPA discloses each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits **(AAPA, paragraph 5, teaches the use of a feedback loop system to keep the power supply current constant to prevent the unauthorized access to the encryption key.)**, the activity information indicative of whether each of the processing circuits generates a logic level transition **(AAPA, paragraphs 3 and 4, also teach monitoring the activity level of a cryptographic circuit by monitoring the logic level changes of the circuit.)**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Thüringer by adding the teachings of AAPA. Thüringer teaches masking the power supply current by using a loading circuit. AAPA, paragraphs 3-5, teach masking the power supply current by monitoring the logic level changes of the circuit and also by using a feedback loop system. All of these systems are used to mask the power supply current to prevent the unauthorized access to the encryption information that is used in the circuit. It would have been obvious to use one system instead of another or to combine the systems to make it even more secure.

As per claim 11, Thuringer in view of Odinak and AAPA discloses a plurality of activity monitor circuits each coupled to receive the input and output signals of one of the processing circuits **(Figure 2, Thüringer teaches a circuit that takes in a pair of signals and then outputs a pair of signals after processing. Thüringer, col. 2 lines 39-45, discloses the inputting and outputting of Figure 2. Odinak, col. 2 lines 12-26, teaches having multiple current sinks that randomly turn on and off. The combination of the current from all current sinks produces a cloaking current that is not dependant on any secret information. This cloaking current is then used to mask the normal power fluctuations that could be used to determine the secret information. It is also well known that a processing circuit must have input and output signals. AAPA, paragraph 5, also teaches the use of a feedback loop system.)**

As per claims 10 and 12, Thuringer in view of Odinak and AAPA discloses deriving activity information from each pair of processing signals includes generating respective currents proportional to a difference between the input signal and the output signal of each of the pairs of processing signals, and wherein the sum of power supply currents is a sum of the respective currents **(Odinak, col. 2 lines 12-26, teaches having multiple current sinks that randomly turn on and off. The combination of the current from all current sinks produces a cloaking current that is not dependant on any secret information. This cloaking current is then used to mask the normal power fluctuations that could be used to determine the secret information.)**

As per claim 13, Thuringer in view of Odinak and AAPA discloses wherein the current drawing circuit is a digital to analog converter that is configured to convert a digitally coded value into an analog power supply current that is equal to the cloaking current **(Both Thuringer and Odinak teach outputting the masking or cloaking current as an analog signal. If the processing circuits perform the processing and output a digital cloaking current, it would have been obvious to use a digital to analog converter to output the cloaking current as an analog value as taught by Thuringer and Odinak.)**

12. **Claims 2-4** are rejected under 35 U.S.C. 103(a) as being unpatentable over Thüringer in view of Odinak, AAPA, and further in view of NPL by Patterson et al. (Computer Architecture : A Quantitative Approach) pages 134-135 published in 1995, hereinafter referred to as Patterson.

As per claim 2, Thüringer in view of Odinak and AAPA discloses an electronic circuit device according to claim 1 **[See rejection to claim 1 above]**. Thüringer also discloses having combinatorial logic circuits to generate a pair of signals to use for a load circuit to mask the power supply consumption.

However, Thüringer does not specifically teach having a clock or registers.

Thüringer does teach that the "concepts can be realized independently of the construction of the logic (synchronous or asynchronous circuit technique)" **(col. 3 lines 32-34).**

It would have been obvious to one of ordinary skill in the art at the time of the invention to know that a synchronous circuit technique involves the use of a clock **(col. 3 lines 32-34, Thüringer teaches the use of a synchronous circuit, which involves a clock.)**

Furthermore, Patterson discloses the processing unit comprises a clock circuit **(pages 134-135, Patterson teaches having a clock.)**, combinatorial logic circuits and registers clocked by the clock circuit and connected between respective parts of the combinatorial logic circuits **(Figure 3.4, Patterson teaches a processor instruction datapath being pipelined and adding a set of registers between each pair of**

pipeline stages. Patterson also teaches that every pipeline stage is active on each clock cycle. Therefore, the registers must also be controlled by the clock because the values in the registers can change after each pipeline stage.), the pairs of processing signals comprising pairs of input and output signals of the registers **(Figure 3.4, Patterson teaches a set of registers. Each register has a set of signals coming into and going out of the register.)**, the current drawing circuit being arranged to adjust a value of the cloaking current dependent on the activity of the registers at instants synchronized by the clock circuit **(Thüringer, Figure 3 and col. 3 lines 17-25, teaches using a computing element, and monitoring this computing element, to generate the complementary loading current used to mask the measurable power consumption. It is well know in the art that registers are computing elements. Patterson, pages 134-135, teaches using registers as computing elements.)**

Thüringer and Patterson are analogous art because they are from the same field of endeavor of using computer circuitry to perform a set of instructions.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Thüringer’s teachings with the teachings of Patterson because adding the registers between the different combinatorial logic circuits is helpful to transfer data from one combinatorial logic circuit to the next **(Patterson, Figure 3.4, teaches the use of the pipeline registers.)**

As per claim 3, Thüringer in view of Odinak, AAPA, and Patterson discloses an electronic circuit device according to claim 2 **[See rejection to claim 2 above]**, organized as a pipe-line of successive parts of the combinatorial logic circuits **(Thüringer, Figure 3, teaches the use of a pipe-line. The layout of the circuit is such that the output from one set of circuits is the input into another set of circuits and this constitutes a pipe-line.)**, each pair of successive parts coupled via a respective one or respective ones of the registers **(Patterson, Figure 3.4, teaches a processor instruction datapath being pipelined and adding a set of registers between each pair of pipeline stages.)**, the electronic circuit device **(Thüringer, Figures 1-3, teach an electronic circuit.)**, comprising: a plurality of activity monitor circuits **(Thüringer, Figures 2-3, teach a set of circuits that are used to monitor the activity (logic high or low) of the incoming signals and generate a load current to mask the measurable power consumption.)**, each coupled to receive pairs of input and output signals of the respective one or ones of the registers between a respective pair of successive parts of the combinatorial circuits **(Figure 3.4, Patterson teaches a set of registers between each pipeline stage. Each stage in the pipeline is comprised of a set of combinatorial circuits. Each register has a set of signals coming into and going out of the register.)**, and to derive a combined activity signal from the pairs of input output signals **(Thüringer, col. 2 lines 47-60, teaches the circuit determining if the incoming logic signals are high or low. Thüringer, col. 1 lines 46-65, also teaches the load circuit being controlled by at least part of the data processing device. As shown in Thüringer Figure 3, the signals that are**

processed by the data processing device are sent to the circuit arrangement of Figure 2 to generate the complement which is later used to control the load circuit to mask the measurable power consumption.); a plurality of current drawing circuits connected to the power supply connections **(Thüringer, Figure 2, discloses a plurality of processing circuits such as the AND gates. It is inherent that the AND gates are connected to the power supply in order for the circuit to work.)**, each controlled by a respective one of the activity monitor circuits to draw a cloaking current controlled by combined activity signal derived by that respective one of the activity monitor circuits **(Thüringer, col. 1 lines 46-65, teaches the load circuit being controlled by at least part of the data processing device. As shown in Thüringer Figure 3, the signals that are processed by the data processing device are sent to the circuit arrangement of Figure 2 to generate the complement which is later used to control the load circuit to mask the measurable power consumption.)**

As per claim 4, Thüringer in view of Odinak, AAPA, and Patterson discloses an electronic circuit device according to claim 3 **[See rejection to claim 3 above]**, arranged to activate the current drawing circuits in selected clock cycles **(Thüringer, col. 1 lines 28-33 and col. 1 lines 46-65, teach using a load circuit during security-relevant operations to mask the measurable power supply. Patterson, page 134, teaches executing every stage in the pipeline during each clock cycle. Thüringer, col. 3 lines 32-34, also teaches the use of a clock.)**, when the corresponding pipe-line stages process secret information **(Thüringer, col. 1 lines 28-33, teaches using**

the load circuit to mask the measurable power consumption at least during security-relevant operations where the security-relevant operations involve processing secret information as indicated in col. 2 lines 62-67 through col. 3 lines 1-6. Patterson, pages 134-135 and Figure 3.4, teaches the use of pipeline stages.)

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to John B. King whose telephone number is (571)270-7310. The examiner can normally be reached on Mon. - Fri. 7:30 AM - 4:00 PM est..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/John B King/
Examiner, Art Unit 2435

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435